Amendments to the Specification

Paragraph beginning on page 1, line 10

In recent years, the world has witnessed the explosive growth of the Internet. Each year ~~many more~~ additional hosts are added while the number of users seems to ~~be growing~~ grow without limit. The Internet enables communications using different techniques including remote computer login, file transfer, world wide web (WWW) browsing, email, etc. Various protocols have been designed and are in use on the Internet to handle various types of communications. For example, file transfer protocol (FTP) for file transfer, hypertext markup language (HTML) for web traffic, etc. Generally, the protocol related to Internet communications are grouped under the umbrella of the transmission control protocol/internet protocol (TCP/IP) suite of protocols that includes protocols at various layers of the OSI communications stack.

Paragraph beginning on page 1, line 20

A key feature of the Internet is that it is a public network that is accessible by nearly anyone with a computer, telephone line and Internet service provider (ISP) account. A downside to this wide scale public accessibility is that it permits easy access [[to]] for hackers and others intent on carrying out malicious activities against one or more hosts on the Internet. Illegal conduct such as stealing of secret information or the deletion of important files by a malicious user is possible by a hacker that manages to break into a computer of a remote network and succeed to tap communication data. The need for security was addressed by the Internet Architecture Board (IAB) by including security features such as encryption and authentication in IPv6 that permit secure transactions over the Internet.

Paragraph beginning on page 2, line 4

At the same time, the world is witnessing increasing demand for wireless services (i.e. cellular phones, two way pagers, cordless devices, etc.) and personal computing devices such as laptops, PDAs, etc. Many of these personal computing devices incorporate wireless communications circuitry to enable them to communicate via wireless networks (e.g., cellular or other broadband schemes) to WAN networks such as the Internet. Thus, more and more PDAs and cellular telephones are being ~~connecting~~ connected to the Internet thus exposing these devices to security risks. Preferably, these devices employ some type of firewall to protect against unauthorized access to the device. Most firewalls today, however, are implemented in software and

require the computing resources of an entire desktop computer, making their use in a portable computing device such as cellular telephone or PDA very costly or impractical.

Paragraph beginning on page 3, line 2

The present invention provides a novel and useful virtual private network (VPN) mechanism for providing the necessary security related parameters to perform encryption/decryption and authentication. The VPN mechanism is adapted to be suitable for implementation in hardware at relatively low cost thus enabling cost effective incorporation of the invention in [[to]] portable electronic ~~communications device~~ communication devices such as cellular telephones, personal digital assistants (PDAs), laptop computers, etc. in connecting to the Internet or other wide area network.

Paragraph beginning on page 10, line 3

The present invention provides a novel and useful virtual private network (VPN) mechanism for providing the necessary security related parameters to perform encryption/decryption and authentication. The VPN mechanism is adapted to be suitable for implementation in hardware at relatively low cost thus enabling cost effective incorporation of the invention in [[to]] portable electronic ~~communications device~~ communication devices such as cellular telephones, personal digital assistants (PDAs), laptop computers, etc. in connecting to the Internet or other wide area network. The present invention can be used in conjunction with a hardware-or software based firewall in portable computing devices such as cellular telephones and wireless connected PDAs that are adapted to connect to the Internet. The VPN mechanism of the present invention may also be implemented in software or a combination of hardware and software.

Paragraph beginning on page 13, line 20

The security association processor comprises a SA recognition module 76, main SA processing module 78 incorporating a CPU interface 79, SA management module 80, hash table 82, SA Least Recently Used (LRU) circuit 84 and SA database 86 all of which are in communication over a bus with the security engines 90 in the VPN security processor and the packet builder.

Paragraph beginning on page 14, line 14

In operation, the VPN module is operative to open new [[SA]] SAs including establishing connections to the LRU and hash linked lists, determining to which SA an input packet corresponds to, updating the state of the SA after successful processing of a packet and removing unused SAs from the connection table. Note that the SA database is implemented and arranged such that SA recognition and pointer management can be easily and quickly performed.

Paragraph beginning on page 15, line 1

The main SA processing module also is adapted to count the number of bytes transferred on each SA per packet and generate a notification when the lifetime for a SA overflows. ~~Upon~~ If an overflow detected, the manager closes (i.e. kills) the SA.

Paragraph beginning on page 16, line 1

It is first checked whether the packet received is an inbound or outbound packet (step 110). If it is an outbound packet, it is then checked whether a SA was found by the dynamic filter (step 154). Normally, the dynamic filter searches its database for a session with a socket that matches that of the received packet. For each session there is stored a corresponding SA in the session database in the dynamic filter. Upon finding a matching session, the corresponding SA is read out and input to the SA processor. The operation of the dynamic filter is described in more detail in U.S. ~~Application Serial~~ Patent No. ~~09/851,768, filed May 9, 2001~~ 6,816,455, entitled "Dynamic Packet Filter Using Session Tracking," ~~similarly assigned and~~ incorporated herein in its entirety.

Paragraph beginning on page 23, line 4

All of the upper flags are set by the CPU and read by the SA processor. The EMP flag can also be set by the SA processor. The SA processor sets this bit to a one when the SA is empty, i.e. invalid. The CPU sets this bit to zero when the SA is valid. The IPM bits indicate the specific IPSec mode, i.e., ESP, ESP/AU, AU only, transport, tunneling, etc. The last three IPSec modes can optionally be used to implement additional security standards, such as Secure Sockets Layer (SSL), to encrypt a certain file, etc. In these modes, the VPN engine is used stand alone without the packet building functionality. Thus, the VPN engine functions as a software accelerator implementing DES/3DES encryption/decryption engine mode (IPM=1100), SHA-1/MD-5 authentication engine mode (IPM=1011) or both encryption and authentication engine mode (IPM=1101).

Paragraph beginning on page 24, line 20

The ARW bits indicate the size of the anti-replay window if it exists. The HLD bit indicates not to delete a particular SA. This flag protects a SA entry from being deleted by the SA processor hardware. The MAN bit indicates whether there is manual keying for the SA. If manual keying is configured, the sequence rolls over when 0xFFFFFFFF is reached since manual keys are not allowed to be deleted by the SA processor. The SAL bit indicates whether the SA lifetime is measured by time or data, i.e. in seconds or 64 bytes units. The SOH bit indicates whether the lifetime is a soft or hard lifetime. The SLT bit indicates that a soft overflow has occurred in the soft lifetime. The SEQ bit indicates that a soft overflow has occurred in the SA sequence. Note that the ARW, HLD, MAN,

SAL and SOH flags are set by the CPU and read by the SA processor. The SLT and SEQ flags are set by the SA processor and read by the CPU. Unless the HLD or MAN flag is set, the SA is deleted upon sequence overflow (0xFFFFFFFF).

Paragraph beginning on page 29, line 32

In another embodiment, a computer is operative to execute software adapted to perform the VPN mechanism of the present invention or any portion thereof such as the security association processor. A block diagram illustrating an example computer processing system ~~to platform~~ adapted to perform the VPN mechanism of the present invention is shown Figure 18. The system may be incorporated within a communications device such as a PDA, cellular telephone, cable modem, broadband modem, laptop, PC, network transmission or switching equipment, network device or any other wired or wireless communications device. The device may be constructed using any combination of hardware and/or software.